



CVE-2020-7245

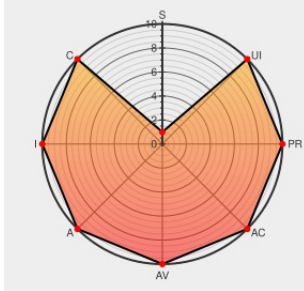
Published on: 01/23/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:53 PM UTC

CVE-2020-7245

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Ctfd](#) from [Ctfd](#) contain the following vulnerability:

Incorrect username validation in the registration process of CTfD v2.0.0 - v2.2.2 allows an attacker to take over an arbitrary account if the username is known and emails are enabled on the CTfD instance. To exploit the vulnerability, one must register with a username identical to the victim's username, but with white space inserted before and/or after the username. This will register the account with the same username as the victim. After initiating a password reset for the new account, CTfD will reset the victim's account password due to the username collision.

CVE-2020-7245 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Strip spaces on registration and refine password reset by GoldHost	Exploit-Database	MISC

Strip spaces on registration and refine password reset by ColdHeat · Pull Request #1218 · CTFd/CTFd · GitHub

Third Party Advisory

github.com

text/html

MISC

github.com/CTFd/CTFd/pull/1218

Release 2.2.3 · CTFd/CTFd · GitHub

Release Notes

github.com

text/html

MISC

github.com/CTFd/CTFd/releases/tag/2.2.3

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	CTfd	CTfd	All	All	All	All

cpe:2.3:a:ctfd:ctfd:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→